CRIMINAL JUSTICE CONNECTIONS

July/August 2014
Volume 21 Issue 6

An employee publication of the
Texas Department of Criminal Justice

Policies and Benefits

Information security: don't fall for tech-support phone scams

As automated information security systems improve, cyber criminals are shifting their attacks to target individual computer users, and it's becoming more common for criminals to call potential victims on the phone in an attempt to run a common tech-support con game. Here's what you can do to avoid being scammed.

Most phone scams are designed to convince an individual to disable their computer system's built-in security. A caller might say they are associated with Microsoft or another legitimate company. They tell you there is a problem with your computer and it may be infected with a virus. They are calling to investigate the problem and offer to help you secure your computer. Then, they use technical jargon while asking you to perform a series of confusing steps on your computer. Ultimately, they convince you that your computer is infected and scare you into disabling security programs or installing their product.

Some scammers may ask you to download and install a program from their website or use online services that give them remote access to your computer so they can troubleshoot and confirm the problem. These tools are usually legitimate remote access tools, such as LogMeIn.com or ShowMyPC.com, so your antivirus software most likely will not flag them. While speaking with you on the phone, the scammer will walk you through your computer's programs and settings. The caller may even begin to disable legitimate security services, claiming they are actually malicious programs. By disabling your computer's software, they are attempting to frighten you into believing that your computer is infected and the only way you can fix the problem is by installing their product. Their ultimate goal is to gain control of your computer and get your money or harvest confidential information.

Remember, everything these criminals are telling you is a lie; do not fall for such attacks. Criminals use the telephone instead of e-mail because there is no technical protection from phone scams and con games. Phone calls are a powerful way to convey emotion and a sense of urgency, and scammers rely on that to gain your cooperation.

It's important to learn to recognize the difference between a legitimate service provider and a phone scammer. Here are some key steps you can take to protect your confidential computer data.

- When someone asks you for information over the phone or asks you to take an action, be suspicious and confirm the person's identity first. Ask what company the person works for. If you have never heard of the company before, then there is a good chance this is an attack. If this is a legitimate company you know, then simply tell the person this is not a good time for you to talk. Ask for a name and employee number and explain that you will call back. Then go to the organiza-

Continued on page 2

July/August 2014
Volume 21 Issue 6

Continued from page 1

tion's website, get the phone number from there and call the company back.

- If the person calling is creating a sense of urgency or creating tremendous pressure for you to take action right away, this is most likely a scam. Do not trust them.

- Do not rely on caller-ID systems to authenticate the source of the call. It is easy for criminals to fool caller-ID systems so they can pretend to be calling from a legitimate company.

- Never give your password out over the phone at home. At work, Information Technology (IT) staff will rarely ask for your password, and if they do, be sure you know they are actually an IT employee.

- Never give out information that someone should already possess. For example, if your bank is calling you, the caller should already have your account number.

The IT department's Computer Help Desk has an administrative login which allows them to do their work. If they ask if you know your password, say you do, but do not give them your password. They are only ensuring that you will be able to access the system on your own after the help call has ended. If they need your password, they will specifically ask for it. In any event, you should always change your password immediately after a computer problem has been resolved.

If you are unsure of the individual calling, do not feel guilty for asking them questions. It is their responsibility to identify themselves. Within TDCJ, if you feel that the individual is trying to scam you, please inform the Information Security Office so that appropriate actions can be taken.

If you have questions, comments or suggestions regarding TDCJ Information Security, please contact the Information Security Department at: iso@tdcj.texas.gov or 936-437-1800.●